The 10 Immutable Laws of Network Security

Law #1: If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore.
Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore.
Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
Law #4: If you allow a bad guy to run active content in your website, it's not your website any more.
Law #5: Weak passwords trump strong security.
Law #6: A computer is only as secure as the administrator is trustworthy.
Law #7: Encrypted data is only as secure as its decryption key.
Law #8: An out-of-date anti-malware scanner is only marginally better than no scanner at all.
Law #9: Absolute anonymity isn't practically achievable, online or offline.
Law #10: Technology is not a panacea.

The Laws Explained (details)

Law #1: If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore
It's an unfortunate fact of computer science: when a computer program runs, it will do what it's programmed to do, even if it's programmed to be harmful. When you choose to run a program, you are making a decision to turn over a certain level of control of your computer to it -- often anything up to the limits of what you yourself can do on the computer (and sometimes beyond). It could monitor your keystrokes and send them to criminals eager for the information. It could open every document on the computer, and change the word "will" to "won't" in all of them. It could send rude emails to all your friends. It could install a virus. It could create a "back door" that lets someone remotely control your computer. It could relay a bad guy’s attack on someone else’s computers. Or it could just reformat your hard drive.
That's why it's important never to run a program from an untrusted source, and to limit the ability of others to make that decision for you on your computer. There's a nice analogy between running a program and eating a sandwich. If a stranger walked up to you and handed you a sandwich, would you eat it? Probably not. How about if your best friend gave you a sandwich? Maybe you would, maybe you wouldn't—it depends on whether she made it or found it lying in the street. Apply the same critical thought to a program that you would to a sandwich, and you'll usually be safe.

Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore
In the end, an operating system is just a series of ones and zeroes that, when interpreted by the processor, cause the computer to do certain things. Change the ones and zeroes, and it will do something different. Where are the ones and zeroes stored? On the computer, right along with everything else! They're just files, and if other people who use the computer are permitted to change those files, it's "game over.”
To understand why, consider that operating system files are among the most trusted ones on the computer, and they generally run with system-level privileges. That is, they can do absolutely anything. Among other things, they're trusted to manage user accounts, handle password changes, and enforce the rules governing who can do what on the computer. If a bad guy can change them, the now-untrustworthy files will do his bidding, and there's no limit to what he can do. He can steal passwords, make himself an administrator on the computer, or add entirely new functions to the operating system.
To prevent this type of attack, make sure that the system files (and the registry, for that matter) are well protected. In modern operating systems, default settings largely prevent anyone but administrators from making such bedrock changes. Preventing rogue programs from gaining administrative-level access is the best way of protecting the operating system. That’s best accomplished by not operating your computer from an account with administrative privileges except when specific tasks make it absolutely necessary – and logging out of that high-privilege mode as quickly as possible once your task is complete. Home users should consider creating an “everyday” account set to operate with standard-level user permissions. On those relatively rare occasions when you really do need to make big changes, you can log into the administrative account, do whatever needs to be done, and switch back to the safer account when you’re finished.

Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore
Oh, the things a bad guy can do if he can lay his hands on your computer! Here's a sampling, going from Stone Age to Space Age:
He could mount the ultimate low-tech denial of service attack, and smash your computer with a sledgehammer.
He could unplug the computer, haul it out of your building, and hold it for ransom.
He could boot the computer from removable media, and reformat your hard drive. But wait, you say, I've configured the BIOS on my computer to prompt for a password when I turn the power on. No problem – if he can open the case and get his hands on the system hardware, he could just replace the BIOS chip. (Actually, there are even easier ways).
He could remove the hard drive from your computer, install it into his computer, and read any unencrypted data.
He could duplicate your hard drive and take it back to his lair. Once there, he'd have all the time in the world to conduct brute-force attacks, such as trying every possible logon or decryption password. Programs are available to automate this and, given enough time, it's almost certain that he would succeed. Once that happens, Laws #1 and #2 above apply.
He could add a recording device or transmitter to your keyboard, then monitor everything you type including your passwords.
Always make sure that a computer is physically protected in a way that's consistent with its value—and remember that the value of a computer includes not just the value of the hardware itself, but the value of the data on it, and the value of the access to your network that a bad guy could gain. At a minimum, business-critical computers such as domain controllers, database servers, and print/file servers should always be in a locked room that only people charged with administration and maintenance can access. But you may want to consider protecting other computers as well, and potentially using additional measures to guard their physical integrity.

If you travel with a laptop or other portable computer, it's absolutely critical that you protect it. The same features that make them great to travel with – small size, light weight, and so forth – also make them easy to steal. There are a variety of locks and alarms available for laptops, some models let you remove the hard drive and carry it with you, and almost all can be used with extremely small, extremely portable storage – e.g. USB thumb drives – for storing your data while you travel. You also can use features such as drive encryption available in most modern operating systems to mitigate the damage if someone succeeded in stealing the computer, or to retain some confidence in its protection if it's taken from you in an unexpected bag check or unfriendly border crossing. If the computer walks off or is lost, you'll still need to address the loss of the hardware, but it'll be harder for your data to be disclosed without your knowledge. But the only way you can know with 100% certainty that your data is safe and the hardware hasn't been tampered with, is to keep them on your person at all times while traveling.

Law #4: If you allow a bad guy to run active content on your website or online application, it's not your website any more

In Law #1, a bad guy tricks you into downloading a harmful program and running it, giving him control over your computer and its data – at least as much control as you had. But what about the reverse: if he can upload active content – programs, scripts, or even documents and pictures designed to crash peoples' computers in specific ways – and have them served from your website or online application? Your site becomes his platform for reaching out to capture data from site visitors or harm their computers, or reaching inward towards other systems that support your site.

If you run a website or hosted applications, you need to limit what visitors can do. Some sites provide an open forum for people to upload and distribute software, code or configurations – and that's fine as long as visitors understand Law #1 and the risks that come along with their downloads. But if the bad guy's uploaded programs actually run on your server or in the browser of visitors, he effectively own your site and can impersonate you. Worse, the bad guy could gain your rights to the underlying systems, and might find a way to extend his control to the servers, data storage or network itself. If your site is on shared infrastructure or a cloud-based service, this can put other sites and data at risk, and potentially create interesting liabilities for yourself and other people.

A properly administered site host or cloud service will have taken many of these risks into account and will disallow scripts or programs uploaded to the service from affecting other accounts that happen to share the same resources. Just the same, you should only allow a program to run on your site or as part of your application if you wrote it yourself or if you trust the developer who wrote it, and make sure your operations and maintenance processes don't run afoul of the host administrator's security policies.

Law #5: Weak passwords trump strong security

The purpose of having a logon process is to establish who you are. Once the operating system knows who you are, it can grant or deny requests for system resources appropriately. If a bad guy learns your password, he can log on as you. In fact, as far as the operating system is concerned, he is you. Whatever you can do on the system, he can do as well, because he is you. Maybe he wants to read sensitive information you've stored on your computer, like your e-mail. Maybe you have more privileges on the network than he does, and being you will let him do things he normally couldn't. Or maybe he just wants to do something malicious and blame it on you. In any case, it's worth protecting your credentials.

Always use a password on your computer—it's amazing how many accounts have blank passwords. And develop a complex one. ***Don't use your dog's name, your anniversary date, the name of the local football team, or QWERTY / 12345 / other basic keyboard patterns – and avoid using single "dictionary words" (that is, words that can be looked up in the dictionary)*. *And don't use the word "password!"*** Build a password that has a mix of upper- and lower-case letters, numbers, punctuation marks, and so forth.

Make it as long as possible; consider using two words in combination. (If you speak multiple languages, you might choose to mix tongues in your password for extra complexity.) And change it often.

Once you've picked a strong password, handle it appropriately. Don't write it down. If you absolutely must write it down, at the very least keep it in a safe, a locked drawer, or perhaps deep in your wallet—the first thing a bad guy who's hunting for passwords will do is check for a yellow sticky note on the side of your screen, or in the top desk drawer. Don't tell anyone what your password is, and don't ask for theirs. Managers, kids, and even IT helpdesk staff should rarely if ever ask for your password. Modern operating systems and programs allow you to give other people permission to see and use your files, without giving out your password so they can impersonate you. Remember what Ben Franklin said: two people can keep a secret, but only if one of them is dead.

If you have accounts for multiple computers and online services, you'll need to balance requirements for unique and strong passwords, yet limit how many passwords you have to remember. For accounts that give access to your most critical information – financial accounts, regulated personal data, sensitive work access, and primary email accounts to name a few – use a unique password for each one, and follow their access management policies. If you're awash in multiple accounts that gather little personal information and have low value if lost, such as news sites that require free registration, consider developing one reasonably strong password and reusing it for most or all of them.

Finally, consider using something stronger than – and in addition to – passwords to identify yourself to the system. Windows, for instance, supports the use of smart cards, which significantly strengthens the account checking the system can perform. You may also want to consider biometric products such as fingerprint and retina scanners. "Two-factor authentication" of this sort incorporates not only something you know (your password) but something you own (a card) or even something you are (a person with your unique fingerprint or retina) – dramatically increasing authentication strength.

Law #6: A computer is only as secure as the administrator is trustworthy

Every computer must have an administrator: someone who can install software, configure the operating system, add and manage user accounts, establish security policies, and handle all the other management tasks associated with keeping a computer up and running. By definition, these tasks require that the individual have control over the computer. This puts the administrator in a position of unequalled power. An untrustworthy administrator can negate every other security measure you've taken. He can change the permissions on the computer, modify the system security policies, install malicious software, add bogus users, or do any of a million other things. He can subvert virtually any protective measure in the operating system, because he controls it. Worst of all, he can cover his tracks. If you have an untrustworthy administrator, you have absolutely no security.

When hiring a system administrator, recognize the position of trust that administrators occupy, and only hire people who warrant that trust. Call his references, and ask them about his previous work record, especially with regard to any security incidents at previous employers. If appropriate for your organization, you may also consider taking a step that banks and other security-conscious companies do, and require that your administrators pass a complete background check at hiring time, and at periodic intervals afterward. Whatever criteria you select, apply them across the board. Don't give anyone administrative privileges on your network unless they've been vetted – and this includes temporary employees and contractors.

Next, take steps to help keep honest people honest. Use sign-in/sign-out sheets or log access badge swipes to track who's been in the server room. (You do have a server room with a locked door, right? If not, re-read Law #3). Implement a "two person" rule when installing or upgrading software. Diversify management tasks as much as possible, as a way of minimizing how much power any one administrator has.

Also, don't use the Administrator account—instead, give each administrator a separate account with administrative privileges, so you can tell who's doing what. Many industries require audit logs documenting all activities on covered business systems; audit trails can't stop rogue admins from running amok, but they can record who did what if a problem is discovered later, and enforce a sense of individual accountability. Finally, consider taking steps to make it more difficult for a rogue administrator to cover his tracks. For instance, store audit data on write-only media, or house System A's audit data on System B, and make sure that the two systems have different administrators. The more accountable your administrators are, the less likely you are to have problems.

Law #7: Encrypted data is only as secure as its decryption key
Suppose you installed the biggest, strongest, most secure lock in the world on your front door, but you put the key under the front door mat. It wouldn't really matter how strong the lock is, would it? The critical factor would be the weak way the key was protected, because if a burglar could find it, he'd have everything he needed to open the lock. Encrypted data works the same way—no matter how strong the crypto algorithm is, the data is only as safe as the key that can decrypt it.
Many operating systems and cryptographic software products give you an option to store cryptographic keys on the computer. The advantage is convenience – you don't have to handle the key – but it comes at the cost of security. Simply put, no matter how well the keys are hidden on the system, the software has to be able to find them – and if it can, so can a sufficiently motivated bad guy.
A better solution is to store them in a protected repository. For instance, the Trusted Platform Module (TPM) chip that's present on most computers is designed to strongly protect cryptographic keys, and release them only when a PIN is entered. Smart cards provide similar protection, and their portability means that you can also physically separate them from the computer. But the best "protected repository" is your brain – if the key is a word or phrase, memorize it.

Law #8: An out-of-date malware scanner is only marginally better than no malware scanner at all
Antimalware scanners work by comparing the data on your computer against a collection of malware "signatures." Each signature is characteristic of a particular malware family, and when the scanner finds data in a file, email or elsewhere that matches the signature, it concludes that it's found trouble. It's vital that you keep your malware scanner's signature file up-to-date, as new malware is created every day.
The problem actually goes a bit deeper than this, though. Typically, malware will do the greatest amount of damage during the early stages of its life, precisely because antimalware programs will not be able to detect it, let alone remove it. Once word gets around that new malware is on the loose and people update their signatures, the propagation of the problem falls off as protections spread through the ecosystem. The key is to get ahead of the curve, and have updated signature files on your computer before the malware reaches your machine.
Virtually every maker of antimalware software provides a way to get free updated signature files from their website or from a dedicated update service. In fact, many have "push" services, in which they'll send notification every time a new signature file is released – several times a day, if necessary. Use these services. Also, keep the malware scanner itself—that is, the scanning software that uses the signature files—updated as well. Malware writers regularly develop new techniques and variations that require that scanners change how they do their work.

Law #9: Absolute anonymity isn't practically achievable, online or offline.
All human interaction involves exchanging data of some kind. If someone weaves enough of that data together, they can identify you. Think about all the information that a person can glean in just a short conversation with you: In one glance, they can gauge your height, weight, and approximate age. Your accent will probably tell them what country you're from, and may even tell them what region of the country. If you talk about anything other than the weather, you'll probably tell them something about your family, your interests, where you live, and what you do for a living. It doesn't take long for someone to collect enough information to figure out who you are. If you use any payment system other than cash or any transportation other than your own two feet, you leave a trail of data breadcrumbs that can be used to reconstruct a personally identifiable “portrait” of you with remarkable accuracy. If you crave absolute anonymity, your best bet is to live in a cave and shun all human contact.

The same thing is true of the Internet. If you visit a website, the owner can, if he's sufficiently motivated, find out who you are. After all, the ones and zeroes that make up the Web session have to be able to find their way to the right place, and that place is your computer. There are a lot of measures you can take to disguise the bits, and the more of them you use, the more thoroughly the bits will be disguised. For instance, you could use network address translation to mask your actual IP address, subscribe to an anonymizing service that launders bits by relaying them from one end of the ether to the other, use a different ISP account for different purposes, surf certain sites only from public kiosks, and so on. All of these make it more difficult to determine who you are, but none of them make it impossible. Do you know for certain who operates the anonymizing service? Maybe it's the same person who owns the website you just visited! Or what about that innocuous website you visited yesterday, that offered to mail you a free $10 off coupon? Maybe the owner is willing to share information with other website owners. If so, the second website owner may be able to correlate the information from the two sites and determine who you are. And anonymity is even less achievable when you factor in location data, which is gathered perpetually by mobile phones and often enough by Web sites, mapping your machine’s IP address to a real-world location with pretty decent accuracy.

Does this mean that privacy is a lost cause? Not at all. Governments along with public and private entities continue to wrestle with how best to balance the need for personal data privacy with other concerns. What it means is that the best way for you to protect your privacy on the Internet is the same as the way you protect your privacy in normal life—through your behavior. Read the privacy statements on the websites you visit, and only do business with those whose data-sharing practices you understand and agree with. If sites you visit allow you to determine how and with whom information about you will be shared, learn how to adjust those settings and check yours regularly. If you're worried about cookies, disable them. Most importantly, remember that information shared by or about you online is only as safe as the least protective, least enforced privacy policies and settings with which it comes into contact. But if it's complete and total anonymity you want, better start looking for that cave.

Law #10: Technology is not a panacea
Technology can do some amazing things. Recent years have seen the development of ever-cheaper and more powerful hardware, software that harnesses that hardware to open new vistas for computer users, and services that change our expectations for both, as well as advancements in cryptography and other sciences. It's tempting to believe that technology can deliver a risk-free world if we just work hard enough. However, this is simply not realistic.

Perfect security requires a level of perfection that simply doesn't exist, and in fact isn't likely to ever exist. This is true for software as well as virtually all fields of human interest. Software development is an imperfect science, and all software has bugs. Some of them can be exploited to cause security breaches. That's just a fact of life. But even if software could be made perfect, it wouldn't solve the problem entirely. Most attacks involve, to one degree or another, some manipulation of human nature, a process usually referred to as social engineering.

Raise the cost and difficulty of attacking security technology, and bad guys respond by shifting their focus away from the technology and toward the human being at the console.

It's vital that you understand your role in maintaining solid security, or you could become the chink in your own systems' armor.

The solution is to recognize two essential points. First, security consists of both technology and policy—that is, it's the combination of the technology and how it's used that ultimately determines how secure your systems are. Second, security is a journey, not a destination—it isn't a problem that can be "solved" once and for all, but a constant series of moves and countermoves between the good guys and the bad guys. The key is to ensure that you have good security awareness and exercise sound judgment. There are resources available to help you do this. The Technet website, for instance, has hundreds of white papers, best practices guides, checklists and tools, and we're developing more all the time. Combine great technology with sound judgment, and you'll have more effective security.